Noise-Tolerant Quantum Oracles (New Aspects of Theoretical Computer Science)

AUTHOR(S):

Putra, Raymond H.; Iwama, Kazuo; Yamashita, Shigeru

数理解析研究所講究録 1325 巻 2003 年 33-38

Noise–Tolerant Quantum Oracles

京都大学・情報学研究科 レイモンド・H・プテラ (Raymond H. Putra)
Graduate School of Informatics
Kyoto University

Kazuo Iwama†, Raymond H. Putra† and Shigeru Yamashita‡
†Graduate School of Informatics, Kyoto University
‡NTT Communication Science Laboratories, NTT Corporation
Quantum Computation and Information, ERATO-JST
E-mail: {iwama, raymond, ger}@kuis.kyoto-u.ac.jp.

1 Introduction

There are several situations where we can get only a noisy Boolean value for each variable x_i, $1 \leq i \leq N$, when computing a Boolean function $f(x_1, x_2, \ldots, x_N)$. Suppose, for example, that the function f is the Boolean OR of three variables, i.e., $f = x_1 \vee x_2 \vee x_3$. Also suppose that we can know the value a_i (= 0 or 1) of each x_i only through an ϵ-biased oracle $O(i)$ such that:

$$O(i) = \begin{cases} a_i & \text{with probability } \frac{1}{2} + \epsilon, \\ \overline{a_i} & \text{with probability } \frac{1}{2} - \epsilon. \end{cases}$$

In this situation, our natural goal is to obtain the value of $f(a_1, a_2, a_3)$ with a high (say, constant) probability and with the smallest number of oracle calls. For the above particular example, one simple algorithm is to call each $O(i)$ k times and to guess the value of a_i by majority. It is not hard to see that we need $\Omega(\frac{1}{\epsilon^2})$ oracle calls, which we call the *query complexity*, to decide $f(a_1, a_2, a_3)$ with probability one half. Thus, the query complexity obviously depends on the value of ϵ. (A little surprisingly, there are relatively a few proven results in the quantum setting such as [AC02]. Note that many other studies assume that ϵ is a constant, which disappears in the query complexity under the big-O notation [SC02, BKW00].)

In this paper, we investigate such a query complexity in the quantum setting. For the definition of ϵ-biased *quantum* oracles O, we use a model similar to [AC02], namely, if we apply O to $|i\rangle |0^m\rangle |0\rangle$ and measure the last qubit, yielding $w = 0$ or 1, then $Pr[w = a_i] \geq \frac{1}{2} + \epsilon$ for all $1 \leq i \leq N$. It should be noted that this definition describes what should happen if we would *measure* the key bit; we do not have to do so when making each oracle call. Since O is a unitary transformation, $O|i\rangle |0^m\rangle |0\rangle$ must be written in the form of

$$|i'\rangle (\alpha_i |v_i\rangle |a_i\rangle + \beta_i |w_i\rangle |\overline{a_i}\rangle), \qquad (1)$$

where $\alpha_i^2 \geq \frac{1}{2} + \epsilon$ for all i. Unfortunately, it is not clear if we can get any interesting results under this definition. However, a big change occurs if we consider a subclass of this model.

Our Results We impose the following restrictions to (1): (i) $\alpha_i = \alpha = \sqrt{\frac{1}{2} + \epsilon}$, $\beta_i = \beta = \sqrt{\frac{1}{2} - \epsilon}$ for all $1 \leq i \leq N$ and both α and β are real numbers. (Namely, the bias does not depend on each variable.) (ii) $i = i'$ and $v_i = w_i = 0^m$. (Namely, all input and work qubits must be reset after oracle computation.) For such an oracle O, denoted by O_ϵ, we can show that the query complexity does *not* depend on ϵ. More formally, suppose that there is a quantum algorithm A which computes $f(a_1, \ldots, a_N)$ using $T(N)$ queries of the standard noise-free oracle. Then, for any $0 \leq \epsilon \leq \frac{1}{2}$ there exists a quantum algorithm A' which computes $f(a_1, \ldots, a_N)$ using O_ϵ such that its query complexity is $O(T(N))$ with high probability. Note that the result even holds for $\epsilon = 0$. The size of A' does not increase too much; it is polynomial if the size of A is polynomial. Furthermore, it is not necessary to know the value of ϵ to design A'. A typical example is the OR function for which $O(\sqrt{N})$ ϵ-biased oracle calls are enough for any $0 \leq \epsilon \leq \frac{1}{2}$.

This result can be extended to other kinds of oracles such as the so-called inner product (IP) oracles [AC02]. In some cases, we can relax the conditions (i) and (ii). For example, if $T(N) = O(1)$, then (i) is not necessary and (ii) can also be weakened. For the GL Problem discussed in [AC02], our query complexity is $O(1)$ while their complexity is $O(\frac{1}{\epsilon^2})$.

We also show the followings when we use a quantum noisy oracle defined as (1): (i) any quantum algorithm solving the GL problem requires either

$\Omega(\sqrt{N})$ EQ queries or $\Omega(\frac{1}{\sqrt{\epsilon}})$ IP queries, and (*ii*) $\Omega\left(\frac{1}{\epsilon}\right)$ EQ queries are necessary for any quantum algorithm solving the GL problem.

Combining the above results, we show implicitly the difficulty of *clearing auxiliary qubits* for a certain case. That is, when we are given a noisy IP oracle as (1) and an EQ oracle, then $\Omega\left(\frac{1}{\epsilon}\right)$ EQ queries and $\Omega(\frac{1}{\sqrt{\epsilon}})$ IP queries are necessary for clearing the auxiliary qubits of the outcome of the given IP oracle.

2 Oracle Models

Based on the idea of [AC02], our oracle with respect to a Boolean function $f(x)$ is defined as follows. One can see that the oracle in the previous section which returns the value of x_i is a special case.

Definition 1 *A quantum oracle with bias ϵ is a unitary transform O on $n+m+1$ qubits which satisfies the following two properties.*

1. *If the last qubit of $O|x\rangle|0^m\rangle|0\rangle$ is measured, yielding the value $w \in \{0,1\}$, then $Pr[w = f(x)] \geq \frac{1}{2}+\epsilon$ for any $x \in \{0,1\}^n$.*
2. *For any $x \in \{0,1\}^n$ and $y \in \{0,1\}^{m+1}$, the state of the first n qubits of $O|x\rangle|y\rangle$ is $|x\rangle$.*

Since O is a unitary transform, $O|x\rangle|0^m\rangle|0\rangle$ must be written as

$$|x\rangle\left(\alpha_x|v_x\rangle|f(x)\rangle + \beta_x|w_x\rangle\left|\overline{f(x)}\right\rangle\right).$$

In this paper, we consider a subclass of this model, which we call RE (resettable and with equal amplitudes) oracles.

Definition 2 *An RE oracle with bias ϵ, denoted by O_ϵ, is a unitary transform such that*

$$O_\epsilon|x\rangle|0^m\rangle|0\rangle = |x\rangle|0^m\rangle\left(\sqrt{\tfrac{1}{2}+\epsilon}\,|f(x)\rangle + \sqrt{\tfrac{1}{2}-\epsilon}\left|\overline{f(x)}\right\rangle\right),$$

where $0 \leq \epsilon \leq \frac{1}{2}$ is a real number.

It is well known that the resettability condition can always be met by doubling the circuit size if the answer bit is always $|0\rangle$ or $|1\rangle$ or if $\epsilon = \frac{1}{2}$. However, it is not known with the best knowledge of the authors if this is true in general.

By Definition 2, it is straightforward to obtain the following lemma by the basic property of unitary transformation:

Lemma 1 *The unitary transformation O_ϵ which satisfies the Definition 2 is either*

$$O_\epsilon|x\rangle|0^m\rangle|0\rangle = |x\rangle|0^m\rangle\left(\sqrt{\tfrac{1}{2}+\epsilon}\,|f(x)\rangle + \sqrt{\tfrac{1}{2}-\epsilon}\left|\overline{f(x)}\right\rangle\right), \quad (2)$$

$$O_\epsilon|x\rangle|0^m\rangle|1\rangle = |x\rangle|0^m\rangle\left(\sqrt{\tfrac{1}{2}+\epsilon}\left|\overline{f(x)}\right\rangle - \sqrt{\tfrac{1}{2}-\epsilon}\,|f(x)\rangle\right), \quad (3)$$

or

$$O_\epsilon|x\rangle|0^m\rangle|0\rangle = |x\rangle|0^m\rangle\left(\sqrt{\tfrac{1}{2}+\epsilon}\,|f(x)\rangle + \sqrt{\tfrac{1}{2}-\epsilon}\left|\overline{f(x)}\right\rangle\right), \quad (4)$$

$$O_\epsilon|x\rangle|0^m\rangle|1\rangle = |x\rangle|0^m\rangle\left(-\sqrt{\tfrac{1}{2}+\epsilon}\left|\overline{f(x)}\right\rangle + \sqrt{\tfrac{1}{2}-\epsilon}\,|f(x)\rangle\right). \quad (5)$$

In this paper, without loss of generality we use the first one, i.e., (2) and (3).

3 Main Results

3.1 Phase–Change Oracles

We have defined a quantum oracle O_ϵ as an oracle which returns the answer by XOR-ing it with the last qubit. It is known [Amb02, BS02] that this type of quantum oracles are fundamentally equivalent to quantum oracles which reply queries by changing the phase, if the oracle is noise-free. Its ϵ-biased version, denoted by $\tilde{O}_\epsilon$, is given as follows.

$$\tilde{O}_\epsilon|x\rangle|0\rangle = |x\rangle\left((-1)^{f(x)}\sqrt{\tfrac{1}{2}+\epsilon}\,|0\rangle + \sqrt{\tfrac{1}{2}-\epsilon}\,|1\rangle\right), \quad (6)$$

$$\tilde{O}_\epsilon|x\rangle|1\rangle = |x\rangle\left(\sqrt{\tfrac{1}{2}+\epsilon}\,|1\rangle - (-1)^{f(x)}\sqrt{\tfrac{1}{2}-\epsilon}\,|0\rangle\right). \quad (7)$$

It is said that a quantum oracle O_1 can *simulate* another quantum oracle O_2 if there exist unitary transformations U_1 and U_2 such that $O_2 = U_1 O_1 U_2$. Generally, we would like U_i to have polynomial size and this is true in the following lemma.

Lemma 2 *A quantum oracle O_ϵ is equivalent to $\tilde{O}_\epsilon$, i.e., O_ϵ can simulate $\tilde{O}_\epsilon$ and vice versa.*

In what follows, we always use $\tilde{O}_\epsilon$ which is denoted simply by O_ϵ.

3.2 Simulating Noise–Free Oracles using Noisy Ones

We are now ready for stating our main theorem. Let V be any noise-free quantum oracle which maps $|x,b,z\rangle$ to $(-1)^{b\cdot f(x)}|x,b,z\rangle$, where $x \in \{0,1\}^n$ and z be any qubit strings. Note that V is the standard definition for noise-free oracles which often appears in the literature [Amb02, BS02, Gro96].

Theorem 1 *If there exists a quantum algorithm A solving some problem with probability $1-\delta$ by querying V T times, then instead of querying V, A can solve the same problem with probability $1-\delta$ by querying O_ϵ $O(T)$ times.*

Proof. For simplicity, we omit the description of z since it is left unchanged by the oracle transformation. Suppose that we have a quantum state $|\psi\rangle = \sum_x \gamma_x |x\rangle |0\rangle$ at some moment of the algorithm, where $\sum_x |\gamma_x|^2 = 1$. Then it follows that applying oracle O_ϵ to this $|\psi\rangle$ results in

$$O_\epsilon \sum_x \gamma_x |x\rangle |0\rangle = \sum_x (-1)^{f(x)} \sqrt{\frac{1}{2}+\epsilon}\gamma_x |x\rangle |0\rangle + \sum_x \sqrt{\frac{1}{2}-\epsilon}\gamma_x |x\rangle |1\rangle .$$

Now here comes our key technique, namely, to use a measurement: if the measurement on the last qubit results in the state $|0\rangle$, we know that the quantum state after this measurement is exactly the same as the quantum state after calling V. Otherwise, if the state $|1\rangle$ is measured, we simply need to flip the last qubit to 0 and repeat querying O_ϵ since the previous state $|\psi\rangle$ is completely preserved. Note that the expected number of iteration is constant. Thus, A can query O_ϵ instead of V and the query complexity is roughly the same. □

It might be helpful to see how this algorithm works using a concrete example, i.e., computing the N-bit OR function, $x_1 \vee x_2 \vee \ldots \vee x_N$, using the oracle which returns the value of each variable x_i. This can be viewed as another form of Grover's search algorithm[Gro96]. Thus although any classical algorithm needs $\Omega(N)$ queries, there exists a quantum algorithm with only $O(\sqrt{N})$ queries if the bit-asking oracle is noiseless. This algorithm can be simulated using our noisy oracle as follows, whose query complexity is still $O(\sqrt{N})$:

Algorithm
Step 1. Initialize $(n+1)$-qubits to zero, i.e., $|0^n\rangle |0\rangle$.
Step 2. Apply the Hadamard transform to the first n qubits $(H^{\otimes n} \otimes I_1)$.

$$|0^n\rangle |0\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_i |i\rangle |0\rangle .$$

Step 3. Call the oracle O_ϵ.
Step 4. Observe the last qubit. If it is 0 continue to the next step. Otherwise, flip the last qubit to 0 and go back to Step 3.
Step 5. Apply the Hadamard transform $H^{\otimes n} \otimes I_1$.
Step 6. Perform a conditional phase shift $(2|0\rangle\langle 0| - I_n) \otimes I_1$.
Step 7. Perform the Hadamard transform $H^{\otimes n} \otimes I_1$ and go back to Step 3 if the number of iteration does not suffice.

(End of Algorithm)

3.3 Classical Lower Bounds

In order to obtain the correct value of x_i from a noisy classical oracle with some constant probability, we need to repeat the queries m times for the same x_i. The obvious way to obtain the approximate value of x_i, denoted by $\tilde{x_i}$, is by the majority of m queries outcome. The following theorem states that the majority is optimal.

Theorem 2 ([RS91, SC02]) *For any $0 < \epsilon \leq 1/6$ and $0 < \delta < 1/2$, it holds that any classical algorithm that δ-reliably computes the N-bit OR function requires $\Omega(N \log N/\epsilon^2)$ queries of oracles with bias ϵ.*

4 The Goldreich-Levin Problem

As mentioned previously, our restriction on the resettability and the equality of amplitudes can be relaxed if the number of oracle calls is constant. In this section, we see this by using the Goldreich-Levin Problem. We first give the definition of the problem. For details see, e.g., [Bel99, AC02].

Definition 3 (The Goldreich-Levin Problem) *Given a classical inner product (IP_a) oracle with bias ϵ and a classical equivalence (EQ_a) oracle, the task is to determine $a \in \{0,1\}^n$ with a minimum queries of IP_a and EQ_a. On input $x \in \{0,1\}^n$ which is selected at random, IP_a returns a bit $w \in \{0,1\}$ such that*

$$Pr_x[IP(x) = w = a \cdot x] \geq \frac{1}{2} + \epsilon.$$

EQ_a returns 1 if input bit x is a and 0 otherwise.

[GL89] showed how to solve the problem with queries that is polynomial in n and $1/\epsilon$. Moreover, [AC02] proved the lower bound of queries to be $\Omega(\frac{n}{\epsilon^2})$. Note that the above definition of a noisy classical inner product includes the case when IP_a always returns the false answer for a particular x. Thus, we cannot amplify the correctness probability for a particular x by repeating queries.

Based on the [AC02] definition of a quantum inner product (IP_a) oracle, our restricted version, simply called an IP oracle, is defined as follows.

Definition 4 *A quantum inner product oracle is a unitary transform U_{IP} or its inverse $U_{IP}^\dagger$ on $n+m+1$ qubits such that for all $x \in \{0,1\}^n$,*

$$\begin{aligned} U_{IP}|x\rangle|0^m\rangle|0\rangle &= \alpha_x|x\rangle|v_x\rangle|a\cdot x\rangle + \beta_x|x\rangle|v_x\rangle|\overline{a\cdot x}\rangle, \\ U_{IP}|x\rangle|0^m\rangle|1\rangle &= \alpha_x|x\rangle|v_x\rangle|\overline{a\cdot x}\rangle - \beta_x|x\rangle|v_x\rangle|a\cdot x\rangle, \end{aligned}$$

where α_x and β_x are non-negative real numbers such that

$$\begin{aligned} \frac{1}{N}\sum_{x\in\{0,1\}^n}\alpha_x^2 &\geq \frac{1}{2}+\epsilon, \\ \frac{1}{N}\sum_{x\in\{0,1\}^n}\beta_x^2 &\leq \frac{1}{2}-\epsilon, \end{aligned}$$

and $|v_x\rangle$ is a quantum state which is independent of the content of the last qubit.

Our situation is more complex when considering the Goldreich-Levin problem since the noise rate is not fixed for each query anymore. Moreover, the oracle does not have to reset the second register (but the restriction that it is independent of the answer bit still remains). Nevertheless, if the quantum oracle U_{IP} and U_{EQ} are given, we can obtain a quantum algorithm which solves the GL problem with constant probability and with $O(1)$ queries of U_{IP} and U_{EQ}.

Theorem 3 *There exists a quantum algorithm solving the GL problem with constant probability using U_{IP} and U_{EQ} $O(1)$ times.*

Proof. Based on the idea in [BV97, AC02], the following quantum circuit in Fig. 1 solves the GL problem with probability more than $\frac{1}{4}$ for the given input $|0^n\rangle|0^m\rangle|0\rangle$. In the figure, H and X represents the Hadamard transform and the NOT operation, respectively. $\tilde{U}_{IP}$ and its inverse $\tilde{U}_{IP}^\dagger$ are the oracles obtained from Lemma 2. $\tilde{U}_{IP}$ operates as follows:

$$\begin{aligned} \tilde{U}_{IP}|x\rangle|0^m\rangle|0\rangle &= |x\rangle|v_x\rangle\left((-1)^{a\cdot x}\alpha_x|0\rangle + \beta_x|1\rangle\right), \\ \tilde{U}_{IP}|x\rangle|0^m\rangle|1\rangle &= |x\rangle|v_x\rangle\left(\alpha_x|1\rangle - (-1)^{a\cdot x}\beta_x|0\rangle\right). \end{aligned}$$

After querying $\tilde{U}_{IP}$, we perform a measurement on the last qubit. If it is $|0\rangle$, the computation is continued as shown in the figure. Otherwise, we repeat the computation from the beginning. (This is not harmful since we need only $O(1)$ oracle calls, which is a major difference compared to Theorem 1.)

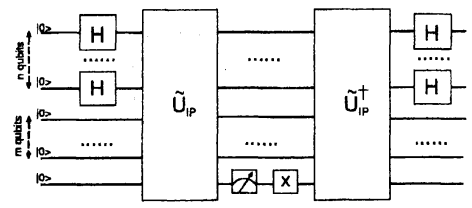

図 1: Quantum Circuit solving the GL problem

The quantum state right before the measurement is as follows:

$$\begin{aligned} &\tilde{U}_{IP}(H_n\otimes I_{m+1})|0^n,0^m,0\rangle \\ &= \frac{1}{\sqrt{N}}\sum_x|x\rangle|v_x\rangle\left((-1)^{a\cdot x}\alpha_x|0\rangle+\beta_x|1\rangle\right), \end{aligned}$$

where H_n and I_{m+1} denote respectively the Hadamard transform on n qubits and the identity operator on $m+1$ qubits. Clearly, the probability of measuring $|0\rangle$ at the last qubit (successful measurement) is $\frac{1}{N}\sum_x\alpha_x^2 = p(0) \geq \frac{1}{2}+\epsilon$. Therefore, after the successful measurement and applying NOT gate, we obtain the quantum state

$$\frac{1}{\sqrt{Np(0)}}\sum_x(-1)^{a\cdot x}\alpha_x|x\rangle|v_x\rangle|1\rangle. \qquad (8)$$

We want to know the amplitude of the basis state $|a,0^m,1\rangle$ at the end of computation. It can be calculated from the inner product of Eq. 8 and the following quantum state:

$$\begin{aligned} &\tilde{U}_{IP}(H_n\otimes I_{m+1})|a,0^m,1\rangle \qquad (9) \\ &= \frac{1}{\sqrt{N}}\sum_x|x\rangle|v_x\rangle\left((-1)^{a\cdot x}\alpha_x|1\rangle-\beta_x|0\rangle\right). \qquad (10) \end{aligned}$$

By simple algebra, the inner product of Eq. 8 and Eq. 9 is

$$\frac{1}{N}\frac{1}{\sqrt{p(0)}}\sum_x\alpha_x^2 = \sqrt{p(0)} \geq \sqrt{\frac{1}{2}+\epsilon}.$$

Therefore, the probability of obtaining $|a,0^m,1\rangle$ is bigger than $\frac{1}{2}$ if the measurement is successful. In total, the probability of obtaining a is bigger than $\frac{1}{4}$. Finally, we can check the answer a with U_{EQ}. This proves the theorem. □

5 Lower Bounds of Quantum Query Complexity

In this section, we consider the lower bounds of query complexity for the Goldreich-Levin problem. Our tool for deriving those lower bounds is the quantum adversary argument which has been proposed by [Amb02] and extended by [BS02].

5.1 Quantum Lower Bounds By Quantum Arguments

The main idea of [Amb02] for deriving the lower bound on the query complexity of quantum oracles is to consider a set of oracles simultaneously. Readers are directed to [Amb02, BS02] for rigorous explanation on the method of quantum adversary argument.

[Amb02, BS02] have shown how to utilize the quantum adversary argument for deriving query complexity of noise-free oracles on various problems. On the contrary, our primary objective is to utilize it to bound the query complexity of noisy oracles, e.g., the Goldreich-Levin problem and noisy inner-product oracles. We show how to utilize the quantum adversary argument for our purpose in the followings.

5.2 Lower Bounds for the Quantum Goldreich-Levin Problem

We want to use the quantum adversary argument [Amb02] to derive the lower bound of the GL problem. However, it turns out that the definition of U_{IP} on the input state other than $|x, 0^m\rangle$ is needed in order to obtain the phase-change oracle. Note that [Amb02] requires that the oracle answers $(-1)^{b\cdot x}|x, b\rangle$ on the input state $|x, b\rangle$. Unless $\alpha_x, \beta_x \in \{0, 1\}$, it is not clear whether we can utilize the quantum adversary argument.

Here, we consider the case when $\alpha_x, \beta_x \in \{0, 1\}$. It is easy to show that by using a U_{IP} and a $U_{IP}^{\dagger}$, we can construct a $\tilde{U}_{IP}$ such that $\tilde{U}_{IP}|x, 0^m\rangle = (-1)^{a\cdot x}|x, 0^m\rangle$ if $\alpha_x = 1$ and $\tilde{U_{IP}}|x, 0^m\rangle = (-1)^{\overline{a\cdot x}}|x, 0^m\rangle$ if $\alpha_x = 0$.

For any two functions f and g, the error rate is defined as

$$error(f, g) = Prob_x[f(x) \neq g(x)].$$

Let f_a be the inner product function defined as $f_a(x) = a \cdot x$. Clearly, the set of all IP oracles with bias ϵ and $\alpha_x, \beta_x \in \{0, 1\}$ is the same with the set F of all Boolean functions with domain $x \in \{0, 1\}^n$ such that for any g in F, there exists an f_a satisfying $error(f_a, g) \leq (\frac{1}{2} - \epsilon)$. We are interested in showing the lower bound of the quantum GL problem in this setting since we can utilize the quantum adversary argument.

Consider a Boolean function $f : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}$ such that:

1. $f(a, b) = 1$ if and only if $a \cdot b = 1$.
2. For $\forall a \neq 0$, $\sum_b f(a, b) \geq \epsilon N$. Otherwise, $f(0, x) = 0$ for all x.

Then, certainly for $\forall a \neq 0$, $error(f, f_a) \leq \frac{1}{2} - \epsilon$, which implies that f is an inner product oracle with bias ϵ. We consider a more restricted Boolean function f as follows.

Lemma 3 *For $\frac{\log N}{N} \leq \epsilon < \frac{1}{4}$, there exists a Boolean function $f : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}$ such that:*

1. *$f(a, b) = 1$ if and only if $a \cdot b = 1$.*
2. *For $\forall a \neq 0$, $\epsilon N \leq \sum_b f(a, b) \leq 3\epsilon N$.*
3. *For $\forall b \neq 0$, $\epsilon N \leq \sum_a f(a, b) \leq 3\epsilon N$.*
4. *$\sum_b f(0, b) = \sum_a f(a, 0) = 0$.*

Now, we are ready for showing the lower bound of the GL problem with regard to the number of IP queries.

Theorem 4 (Bounding IP queries) *Any quantum algorithm solving the GL problem with constant probability requires either $\Omega(\sqrt{N})$ EQ queries or $\Omega(\frac{1}{\sqrt{\epsilon}})$ IP queries.*

We have shown the lower bound of IP queries when the number of EQ queries is $o(\sqrt{N})$. Next, we consider the number of EQ queries regardless of the number of IP queries.

It can be shown that for a Boolean function g which satisfies $error(g, f_a) \leq (\frac{1}{2} - \epsilon)$, the number of such a could be more than one. We want to prove the upper and lower bounds of the number of such a: they could be as large as $O(1/\epsilon^2)$.

For our objective, let us define the following set that consists of all integer $a \in \{0, 1\}^n$ with regard to a Boolean function $g : \{0, 1\}^n \to \{0, 1\}$.

$$D_g^{\epsilon} = \{a \mid \text{error}(f_a, g) \leq \frac{1}{2} - \epsilon\}.$$

The following lemma shows that the size of D_g^{ϵ} can be as large as $\Omega(1/\epsilon^2)$.

Lemma 4 *For any $n \geq 2$, $\exists g : \{0, 1\}^n \to \{0, 1\}$ such that*

$$\frac{1}{32\epsilon^2} \leq |D_g^{\epsilon}| \leq \frac{1}{4\epsilon^2},$$

where $\frac{1}{2\sqrt{N}} \leq \epsilon < \frac{1}{4}$ and $N = 2^n$.

From Lemma 4 we know that $g(x)$, a function of length 2^n, can act as a valid noisy inner product oracle for more than $\frac{1}{32\epsilon^2}$ number of oracles. Therefore,

given this g, any quantum algorithm cannot decide which, of such a lot of possible answers, the real answer of the GL problem unless the EQ oracle is given. Namely, if $a, b \in D_g^\epsilon$ then g is a valid oracle for the noisy inner product oracle correlated to a and b, which implies that given the pair (g, EQ_a) and (g, EQ_b), the algorithm can only utilize the EQ oracle to decide the answer.

Of $O(1/\epsilon^2)$ number of possible answers, the algorithm must decide one true answer, which intuitively means that the algorithm must search in a subspace whose size is $O(1/\epsilon^2)$. Accordingly, the lower bound of search in this subspace is $\Omega(1/\epsilon)$. We show the proof by Ambainis' quantum adversary argument.

We are ready for stating the lower bound of the GL problem with regard to the number of EQ queries.

Theorem 5 (Bounding EQ queries) *Any quantum algorithm solving the GL problem with constant probability requires* $\Omega\left(\frac{1}{\epsilon}\right)$ *EQ queries, for any* $N = 2^n \geq 4$ *and* $\frac{1}{2\sqrt{N}} \leq \epsilon < \frac{1}{4}$.

6 Conclusions and Discussions

In this paper, we have shown that by using a quantum noisy oracle defined as $O|x\rangle|0^m\rangle|0\rangle = \alpha_x|x_1\rangle|y_1\rangle|f(x)\rangle + \beta_x|x_2\rangle|y_2\rangle\left|\overline{f(x)}\right\rangle$, any quantum algorithm solving the GL problem requires either $\Omega(\sqrt{N})$ EQ queries or $\Omega(\frac{1}{\sqrt{\epsilon}})$ IP queries. Also it is shown that $\Omega\left(\frac{1}{\epsilon}\right)$ EQ queries are necessary for any quantum algorithm solving the GL problem.

If we suppose that the above noisy oracle satisfies the conditions that $(i)\alpha_x = \alpha = \sqrt{\frac{1}{2}+\epsilon}$ and $\beta_x = \beta = \sqrt{\frac{1}{2}-\epsilon}$ for all $x \in \{0,1\}^n$, and (ii) $x_1 = x_2 = x$ and $y_1 = y_2 = 0^m$, then it is shown that the quantum query complexity does not depend on the value of ϵ. More formally, any quantum algorithm using a conventional noise-free oracle can be simulated by another quantum algorithm using the above ϵ-biased oracle, for any $0 \leq \epsilon \leq \frac{1}{2}$, with a sacrifice of a constant factor of the query complexity.

Combining the above results, we show implicitly how difficult to *clear auxiliary qubits* for a certain case. That is, when we are given an IP oracle with bias as Definition 4 and an EQ oracle, then $\Omega\left(\frac{1}{\epsilon}\right)$ EQ queries and $\Omega(\frac{1}{\sqrt{\epsilon}})$ IP queries are necessary for clearing the auxiliary qubits of the outcome of the given IP oracle. It should be interesting future work to investigate other cases of clearing auxiliary qubits.

References

[AC02] Mark Adcock and Richard Cleve. A quantum goldreich-levin theorem with cryptographic applications. In *STACS*, 2002. See quant-ph/0108095.

[Amb02] A. Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64:750–767, 2002.

[Bel99] M. Bellare. The goldreich-levin theorem. In *Manuscript*, 1999. Available at http://www-cse.ucsd.edu/users/mihir/.

[BKW00] A. Blum, A. Kalai, and H. Wasserman. Noise-tolerant learning, the parity problem, and the statistical query model. In *STOC*, pages 435–440, 2000.

[BS02] Howard Barnum and Michael Saks. A lower bound on the quantum query complexity of read-once functions. In *quant-ph/0201007*, 2002.

[BV97] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

[GL89] O. Goldreich and L. Levin. Hard-core predicates for any one-way function. In *STOC*, pages 25–32, 1989.

[Gro96] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th ACM Symposium on Theory of Computing*, pages 212–219, 1996.

[RS91] R. Reischuk and B. Schmeltz. Reliable computation with noisy circuits and decision trees In *Proceedings of the 32nd Annual Symposium on Foundations of Computer Science*, pages 602–611, 1991.

[SC02] Mario Szegedy and Xiaomin Chen. Computing boolean functions from multiple faulty copies of input bits. In S. Rajsbaum, editor, *LATIN 2002*, pages 539–553, 2002.